

REMARKS

Claims 1-34, 36-37, 39, 41, 43-46, 49-50, and 52-72 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al. and Cavoukian "Building in Privacy" (Cavoukian). Claims 35 and 48 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S. Patent No. 6,233,618 to Herz. Claims 38 and 51 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S. Patent No. 6,233,618 to Shannon. Claim 40 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S. Patent No. 6,011,858 to Stock et al. Claims 42 and 47 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,256,737 to Bianco et al. in view of U.S. Published Patent Application No. 2001/0011247 A1 to O'Flaherty et al., Cavoukian, and U.S. Patent No. 6,119,096 to Mann et al.

The Examiner rejected claims 35, 38, 48, and 51 over Bianco in view of O'Flaherty and either Herz or Shannon. The Examiner identified both Herz and Shannon as having U.S. Patent No. 6,233,618. In the Office Action dated May 22, 2002, the Examiner identified Herz as U.S. Patent No. 6,029,195. The Office Action is interpreted as intending to use U.S. Patent No. 6,029,195 as the reference entitled Herz in rejecting claims 35 and 48.

Reconsideration is requested. No new matter is added. The rejections are traversed. Claims 1-72 remain in the case for consideration.

REJECTIONS UNDER 35 U.S.C. § 103(a)

Referring to claim 1, the invention is directed toward a method for processing electronic transactions. A user registers with an electronic identifier a registration biometric sample. The user formulates a rule module in a clearinghouse. The rule includes at least one pattern data and at least one execution command. The user is then identified by comparing a bid biometric sample against the biometric samples registered in the electronic identifier. Assuming the user is identified, a rule module of the user is invoked, to execute at least one electronic transmission.

Referring to claim 20, the invention is a system for processing electronic transactions. A biometric input apparatus is used, for providing a registration biometric sample to an electronic identifier during registration, and for providing a bid biometric sample to the electronic identifier when the user wants to execute an electronic transmission. A clearinghouse stores rule modules, combining pattern data with execution commands. An execution module invokes an execution command from a rule module, responsive to the electronic identifier indicating whether the user is successfully identified.

Referring to claim 25, the invention is a method for processing electronic transactions. Two users, a primary and a subordinate, each register biometric samples with an electronic identifier. The users also formulate rule modules, associating pattern data with execution commands. The subordinated user is then identified by the electronic identifier. Assuming the subordinated user is successfully identified, the subordinated user's rule modules are checked to see if they are subordinated to any of the primary user's rule modules. Assuming that one of the subordinated user's rule modules are subordinated to one of the primary user's rule modules, the primary user's rule modules are invoked, thereby executing an electronic transmission.

Referring to claim 54, the invention is a method for processing electronic transactions. A biometric sample is registered. A user-customizable rule module is formed, including at least one pattern data of the user and at least one execution command of the user. A bid biometric sample is compared with the registered biometric sample. If the comparison indicates a successful match, the rule module is invoked.

Referring to claim 63, the invention is directed toward a method for processing electronic transactions. A primary user registers a primary registration biometric sample. A secondary user registers a secondary registration biometric sample. A primary user-customizable rule module, customized to the primary user, is formed, including at least one primary pattern data of the user and at least one primary execution command of the primary user. A secondary user-customizable rule module, customized to the secondary user, is formed, including at least one secondary pattern data of the user and at least one secondary execution command of the secondary user. The secondary rule module is subordinated to the primary rule module. A bid biometric sample taken from the secondary user is compared with at least one previously registered biometric sample. The secondary rule module is determined to be subordinated to the primary rule module. Upon a successful match, the primary rule module is invoked.

Referring to claim 64, the invention is directed toward a device for processing electronic transactions. A biometric input apparatus can provide a bid or registration biometric sample of a user. An electronic rule module clearinghouse can have at least one user-customizable rule module, including at least one pattern data of the user and at least one execution command of the user. An electronic identifier can compare a registration biometric sample with a bid biometric sample. A command execution module can execute at least one execution command.

In all of the foregoing claims, the rule modules is invoked *after* identification of the user.

In contrast to all of the foregoing claims, Bianco teaches a system for authenticating users and granting conditional access to resources. In Bianco, the user provides a user ID. The biometric group to which the user belongs is determined: the biometric policy of the biometric group controlling the authentication of the user. The user's registered biometric sample, associated with the user ID, is also determined. The user's biometric sample is compared with the registered sample. If the samples match according to the biometric policy, then the resources associated with the biometric group may be accessed by the user.

As argued in the Response to the Office Action dated May 22, 2002, there are several differences between the invention and the cited prior art. In the Interview Summary dated August 27, 2003, the Examiner indicated that some of these points were discussed. These points were, in the order mentioned by the Examiner, that identification as described in the claims "is distinct from the authorization and validation techniques of Bianco"; that the rule modules of the claims are user-customizable, whereas Bianco's rule modules are not user-customizable; and that the rules in Bianco are applied pre-authentication, whereas the rule modules of the claims are applied post-identification. In other words, the Examiner agreed with the Applicant that there were at least three points on which the claims could be distinguished over Bianco.

In rejecting the claims in the Office Action dated July 19, 2004, the Examiner has combined Bianco with two additional references: the published patent application of O'Flaherty and the Cavoukian article. The Examiner cites to O'Flaherty only to find support in the prior art for users to be able to customize data in a database. The Examiner's stated reason for including Cavoukian is that Cavoukian teaches biometric identification and authentication.

With reference to Cavoukian, the Applicant believes the articles is self-contradictory. The Applicant acknowledges that Cavoukian describes "biometrics [as] permit[ting]

authentication without identification of the user". But the Applicant is lost in understanding how biometrics could be used in this way. Biometrics are inherently unique to the individual. Thus, a biometric taken from person A will, by definition, be different from a similar biometric taken from person B. Thus, if person A provides the biometric, the only person the biometric should match in the database is person A, meaning that person A has been identified.

The only reasonable interpretation of Cavoukian is that the database storing the "bioscripts" does not associate the "bioscript" with a person's name. But this does not mean that the person is not identified; it only means that the person's name is not directly associated with the "bioscript". Clearly, it would take only a trivial modification of the database to associate the person's name with the "bioscript".

Cavoukian goes on to recite that "the bioscript bears no physical resemblance to the user's actual fingerprint. [The] system does not retain any record, image or template of the individual's actual fingerprint. Therefore, a copy of the fingerprint is never kept on file." But this does not mean that the individual is not uniquely identified in the database when a match is found. This comment only means that the process is not reversible: given a "bioscript", the original fingerprint cannot be derived.

To use Cavoukian's example, she describes the use of biometrics to obtain welfare benefits "anonymously". But the "anonymity" to which Cavoukian refers is not a lack of identification; it is simply denying the name of recipient to the person offering the services. Because the government would not want welfare benefits to be provided to persons not entitled, somewhere there would be a database of biometrics of each legitimate welfare recipient. Each biometric in that database matches a biometric of a person. By not including the name of the welfare recipient, the services provider is not told the *name* of the welfare recipient. But because the government limits welfare benefits, the government would want to know what benefits have been received by which recipients. Thus, the recipient is identified to the government; he is anonymous only to the services provider.

To further elaborate, consider the following. If a person enters a store and says that his name is "John Smith", that name does not uniquely identify him. After all, he could be the John Smith from Los Angeles, CA, or the John Smith from Miami, FL. A name does not necessarily identify; we openly state that names are unique, but when pressed will admit that names are not necessarily unique. That is why, for example, drivers' licenses have unique numbers as issued by the state: the combination of the issuing state and the license number uniquely identify the individual, in a way a name never could.

Thus Cavoukian, despite the language of her article, does not in fact accomplish what she says is her goal. And this makes sense: if an individual cannot be identified, he cannot be personally held responsible for his actions. Such anonymity is unacceptable in most endeavors in life. Thus, Cavoukian's "anonymity" is not true anonymity, whereby a person is never uniquely identified; her "anonymity" is only from the people to whom the identity is not relevant. Against parties that want to know the person's identity, there is no anonymity.

Finally, Cavoukian only explains the benefits of her pseudo-anonymity. She does not explain how it might be implemented. Thus, Cavoukian can at best be said to explain why one might want to implement her scheme; the article fails to enable a system that provides pseudo-anonymity. Because Cavoukian is not an enabling description, its teaching is insufficient to render the claims obvious.

The Applicant also believes the Examiner has failed to make a prima facie argument that the claims are obvious, because the Examiner has failed to present arguments that the prior art teaches biometric identification or applying the rule modules after identification. All arguments made previously are hereby resubmitted.

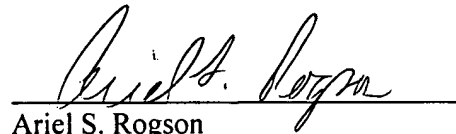
As said in the Response to the Office Action of November 4, 2003, it makes no sense to provide *users* the ability to modify the biometric policies in Bianco. As stated at column 2, lines 61-63, "the biometric policies determine the way or method in which a user is to be authenticated by the system." In other words, the biometric policies specify how the user gains access to resources on the system. If users could modify the biometric policies, they could weaken the security associated with resource access, even to the point of not requiring any security at all. Clearly, a system that allows the user to modify the security associated with accessing a resource is no more secure than a system without any access control at all. Since security and access control are important to Bianco, it would make the Bianco system inoperative for its intended purpose, and therefore would not be obvious to give users the ability to change the security of the system, as would happen if Bianco and O'Flaherty were combined as suggested by the Examiner.

Even if the Examiner intended to analogize between the biometric groups (instead of the biometric policies) of Bianco with rule modules in the claims, the analogy still fails. As argued in the Response to the Office Action dated May 22, 2002, the biometric groups are used to determine which biometric policies to apply in authenticating the user, which means that the biometric groups are used *before* the user is authenticated, and not after the user is identified as claimed.

For the foregoing reasons, reconsideration and allowance of claims 1-72 of the application as amended is solicited. The Examiner is encouraged to telephone the undersigned at (503) 222-3613 if it appears that an interview would be helpful in advancing the case.

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.



Ariel S. Rogson
Reg. No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.
1030 SW Morrison Street
Portland, OR 97205
503-222-3613
Customer No. 20575

I HEREBY CERTIFY THAT
THIS CORRESPONDENCE IS
BEING DEPOSITED WITH THE
UNITED STATES POSTAL
SERVICE AS FIRST CLASS
MAIL IN AN ENVELOPE
ADDRESSED TO:

☐ COMMISSIONER OF PATENTS
AND TRADEMARKS WASHINGTON
D.C. 20231

☒ MAIL STOP *Amedent*
COMMISSIONER FOR PATENTS
BOX 1450
ALEXANDRIA, VA 22313-1450

☐ BOX
COMMISSIONER
FOR TRADEMARKS 2800 CRYSTAL
DRIVE ARLINGTON, VA 22202-3513

ON: *23 Sep 2007*
Ariel S. Rogson